From: DHS Management Communications
Sent: 12 May 2017 19:45:20 -0400
Subject: Ongoing Ransomware Threat

Homeland Security

May 12, 2017

Dear Colleagues,

We are aware of reports of ransomware known as WannaCry affecting multiple global entities. To increase our collective defenses across the Department and Federal networks, we urge all employees to take three actions: (1) do not click on links or download files in emails unless you know for sure that they are intended for you; (2) ensure your personal devices are updated and patched; and, (3) backup your data so you can recover your systems if they become infected. Microsoft released a patch in March that addresses this issue.

Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. The malware spreads by "phishing," luring unsuspecting users to click on infected email attachments and links in emails to launch the attack. Unpatched or out-of-date systems are particularly vulnerable to ransomware.

DHS has previously released information on best practices to address ransomware. That information is available on our website at https://www.us-cert.gov/security-publications/Ransomware.

Sincerely,

Richard Staropoli
Chief Information Officer

With honor and integrity, we will safeguard the American people, our homeland, and our values.

Senior Leadership Brief: WannaCry Ransomware Threat

As of 4:00PM, May 15, 2017

Updates since last report are in red.

Overview

As of 4:00 P.M., DHS has no indications that the Department has been compromised by the WannaCry ransomware. However, the Department is taking precautionary steps to protect the network and the search for indication of compromise continues as more information becomes available.

The National Cyber and Communications Information Center (NCCIC) hosted a follow-up Cybersecurity, Coordination, Assessment and Response (C-CAR) call at 11:00AM this morning. The following is a summarization of this call:

The DHS NCCIC reports that the “WannaCry” ransomware has been reported by over 160 countries. Despite media and open source reporting, this ransomware is not health care centric. In the United States there have been eight (8) private sector victims that have reported infection by the “WannaCry” ransomware. Currently there are no reported incidents of “WannaCry” ransomware in the United States Federal Government sector.

The NCCIC is still working to confirm the initial infection vector for this ransomware. Although the NCCIC has not found the initial vector, they have found the following infection vectors: phishing, executable files and SMB ports open to the internet. Once in the network the ransomware attempts to propagate through SMB traffic. The NCCIC has not found a decryption option for this ransomware at this time.

The NCCIC has also recommended the strict enforcement of SMB traffic and patching of SMBv1 and MS vulnerabilities. The NCATS teams has been scanning for these vulnerabilities and other critical vulnerabilities through their weekly cyber hygiene scans. Please refer to the ESOC operational notes for these cyber hygiene reports. The NCCIC will be releasing a Malware Initial Finding Report (MIFR) later this afternoon on the “WannaCry” ransomware.

Background

DHS is aware of reports of ransomware known as WannaCry affecting multiple global entities. Ransomware is a type of malicious software that infects a computer and restricts users’ access to it until a ransom is paid to unlock it. In this specific instance, the WannaCry ransomware demands $300 worth of bitcoins to decrypt the user’s data or else threatens to keep it encrypted or possibly delete it. The WannaCry ransomware is believed to utilize the NSA-developed exploit named EternalBlue that was released by the hacking group known as the “Shadow Brokers” on April 14, 2017.